Guía de Seguridad de las TIC
CCN-STIC 890A

Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad
(Entidades Locales)



Noviembre 2026

Edita:
centro criptológico nacional
© Centro Criptológico Nacional, 2026

centro criptológico nacional
Firmado digitalmente por CCN
Fecha: 2026.11.12 15:44:55 +01'00'

Fecha de Edición: noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN 4
2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO 4
2.1 SERVICIOS PRESTADOS POR LOS AYUNTAMIENTOS DE HASTA 2.000 HABITANTES 5
2.2 SERVICIOS PRESTADOS POR LOS AYUNTAMIENTOS MAYORES DE 2.000 HABITANTES Y HASTA 5.000 HABITANTES 7
2.3 SERVICIOS PRESTADOS POR LAS ENTIDADES LOCALES MENORES 7
2.4 SERVICIOS PRESTADOS POR AYUNTAMIENTOS (O AGRUPACIONES) DE HASTA 5.000 HABITANTES CON VALORACIÓN MÁS ELEVADA EN ALGUNA DE SUS DIMENSIONES 8
2.4.1 SERVICIOS DE COMPETENCIA MUNICIPAL 8
2.4.2 SERVICIOS DE COMPETENCIA MUNICIPAL INCLUIDOS CON LOS ANEXOS I Y II DE LA DIRECTIVA NIS2 9
3. CONSIDERACIONES DEL SISTEMA DE INFORMACIÓN 10
4. DECLARACIÓN DE APLICABILIDAD 12
4.1 MEDIDAS DE APLICACIÓN 15
5. CRITERIOS DE APLICABILIDAD DE MEDIDAS 17
5.1 [OP.PL.1] ANÁLISIS DE RIESGOS 17
5.2 [OP.ACC.6] MECANISMO DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN) 17
5.3 [OP.EXP.1] INVENTARIO DE ACTIVOS 18
5.4 [OP.EXP.4] MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD 18
5.5 [OP.EXP.7] GESTIÓN DE INCIDENTES 18
5.6 [OP.EXP.8] REGISTRO DE LA ACTIVIDAD 18
5.7 [OP.EXP.9] REGISTRO DE LA GESTIÓN DE INCIDENTES 18
5.8 [OP.EXT.3] PROTECCIÓN DE LA CADENA DE SUMINISTRO 18
5.9 [OP.CONT.2] PLAN DE CONTINUIDAD 19
5.10 [MP.IF.1] ÁREAS SEPARADAS Y CONTROL DE ACCESO 19
5.11 [MP.IF.2] IDENTIFICACIÓN DE LAS PERSONAS 19
5.12 [MP.COM.1] PERÍMETRO SEGURO 20
5.13 [MP.INFO.6] COPIAS DE SEGURIDAD 20

1. INTRODUCCIÓN

En virtud del principio de proporcionalidad y para facilitar la conformidad con el Esquema Nacional de Seguridad (ENS) en determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten de aplicación para una concreta categoría de seguridad.

Un perfil de cumplimiento específico determina una postura de seguridad conforme a un conjunto de medidas de seguridad, comprendidas o no en el Esquema Nacional de Seguridad que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.

De conformidad con lo dispuesto en el ENS (RD 311/2022), los instrumentos normativos previstos (instrucciones técnicas de seguridad y/o guías de seguridad) podrán establecer perfiles de cumplimiento específicos para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables, o los criterios para su determinación.

El Centro Criptológico Nacional, en el ejercicio de sus competencias, ha validado el presente perfil de cumplimiento específico, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, garantizando que las medidas de seguridad implementadas son las necesarias y proporcionales en relación con el contexto de la amenaza, nivel de madurez, riesgo residual asumible y recursos disponibles.

A tal fin, tras un análisis de riesgos contemplando las dificultades, brechas de seguridad, riesgos asociados y las potenciales amenazas a las que se ven expuestas las entidades, organismos u organizaciones; y con el objetivo de garantizar la máxima seguridad de los sistemas de información, se da cumplimiento al mandato impuesto al CCN validando el siguiente Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad (PCE-RFS) que permita la implantación del ENS en las mismas.

2. APLICACIÓN DEL PERFIL DE CUMPLIMIENTO

El objetivo que se persigue con el Perfil de Cumplimiento Específico de Requisitos Fundamentales de Seguridad (PCE-RFS) es posibilitar el cumplimiento del Esquema Nacional de Seguridad (ENS) para categoría BÁSICA de los sistemas de información que dan soporte a la tramitación de servicios e información cuando su valoración, realizada conforme al anexo I del RD ENS 311/2022, es de nivel bajo en todas las dimensiones de seguridad (C- Confidencialidad, I- Integridad, T- Trazabilidad, A- Autenticidad, D- Disponibilidad). Este perfil se destina a entidades, organismos u organizaciones con dificultades para abordar el proceso de adecuación al ENS, con el propósito de facilitar la obtención de la Certificación de Conformidad mediante el cumplimiento de requisitos fundamentales de seguridad empleando la metodología eficiente de certificación en el ENS automatizada en la Plataforma de Gobernanza (µCeENS).

Los certificados expedidos con anterioridad a la fecha de publicación de la actualización de este PCE se mantendrán vigentes hasta su fecha de expiración.

En todo caso, este PCE tiene un carácter transitorio, las entidades dentro del alcance deberán continuar mejorando la seguridad de la información hasta alcanzar el nivel correspondiente a la categorización de sus servicios e información, por lo que, pasado este primer hito en las siguientes certificaciones podrán acogerse al PCE que les corresponda o al modelo estándar de adecuación del ENS.

En caso de que alguna de las entidades dentro del alcance de este PCE preste servicios y/o información cuya valoración, realizada conforme al anexo I del RD ENS 311/2022, sea de nivel medio/alto en alguna de las dimensiones de seguridad (C- Confidencialidad, I- Integridad, T- Trazabilidad, A- Autenticidad, D- Disponibilidad) y quiera aplicar las medidas de este PCE, debe comprometerse a mejorar la seguridad de su sistema de información de forma progresiva hasta alcanzar el nivel de seguridad que le corresponde. En el Anexo III. Compromiso de mejora del sistema de información, se ofrece un modelo para manifestarlo.

Como ejemplo se consideran servicios valorados en algunas de sus dimensiones de nivel medio/alto los siguientes:

- Padrón de habitantes.
- Sociosanitarios (servicios sociales, aplicación ley dependencia, discapacidad…);
- Gestión tributaria.

El alcance será el sistema de información, que da soporte a la tramitación de los servicios y la información, de las siguientes entidades:

- Ayuntamientos de menos 5.000 hab. y agrupaciones de estos municipios (p.e. mancomunidades que presten servicios culturales o deportivos) siempre que presten todos o alguno de los servicios incluidos en el PCE.
- Entidades locales menores (artículo 24 y ss. de la Ley 5/1985, de 2 de abril, reguladora de las Bases de Régimen Local como caseríos, parroquias, aldeas, barrios, anteiglesias, pedanías…) que presten todos o alguno de los servicios incluidos en el PCE.
- Ayuntamientos de mayor tamaño que quieran aplicar las medidas de este PCE como primer paso en su proceso de adecuación al ENS, comprometiéndose a mejorar la seguridad de su sistema de información de forma progresiva hasta alcanzar el nivel de seguridad que les corresponde.

2.1 Servicios prestados por los Ayuntamientos de hasta 2.000 habitantes

A continuación, se describen los servicios e información para los **Ayuntamientos de hasta 2.000 habitantes**, basado en el análisis de los artículos 25, 26 y 27 de la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, considerando que se

trata de entidades locales de pequeño tamaño que por sus características carecen de recursos para prestar servicios adicionales.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que podrían incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
Servicios finalistas				
S01	Urbanismo	Gestión del planeamiento, licencias y autorizaciones, expropiaciones	Planeamiento	Planeamiento
			Licencias y autorizaciones	Expedientes de tramitación: Licencias Urbanismo Expropiaciones
S02	Promoción económica municipal	Diversas actuaciones de promoción del municipio incluyendo las culturales, deportivas, promoción del turismo, económica local	Mercados y abastos	Gestión de actividades comerciales (abastos y mercado)
			Otras acciones de promoción económica (turismo, ferias…)	Gestión de actividades de promoción económica en turismo, ferias, venta ambulante
S03	Actividades culturales y deportivas		Cultura	Gestión de actividades culturales
			Deportes	Gestión de instalaciones deportivas
S04	Servicios funerarios	Servicios de cementerio público		Expedientes adquisición tumbas y personas fallecidas
S05	Medioambiente	Gestión del medioambiente urbano	Control de animales domésticos	Expedientes de registro y control de animales
S06	Personal	Gestión de los RRHH municipales		Expedientes de personal
S07	Servicios Generales (Secretaría _Intervención)	Gestión de los expedientes municipales de diversa índole	Secretaria (informes, control de actas, declaraciones de bienes e intereses, libro decretos)	Informes, actas, declaraciones de bienes, grabaciones de plenos, libro decretos
			Intervención (gestión presupuestaria, cuenta general)	Gestión presupuestaria
			Tesorería (ingresos/pagos)	Ingresos y pagos
			Sistema de cumplimiento: Protección de datos, Transparencia (web, derecho de acceso), participación ciudadana.	Gestión de las obligaciones de la normativa
			Contratación/compras	Expedientes de contratación: propuestas, memoria, ofertas

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que podrían incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
			Archivo	Archivo de expedientes municipales

2.2 Servicios prestados por los Ayuntamientos mayores de 2.000 habitantes y hasta 5.000 habitantes

A continuación, se describen **otros servicios adicionales a los indicados en el apartado anterior que pueden prestar los Ayuntamientos de más de 2.001 hab**. En este caso se toma como referencia también la sentencia del Tribunal Supremo Sala de lo Contencioso-Administrativo, (Sección Quinta) núm. 1.642/2024, de 16 de octubre (ECLI:ES:TS:2024:5003, donde se indica que el alcantarillado es obligatorio para los Ayuntamientos que cuenten con núcleos de población superiores a los 2.000 habitantes):

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que podrían incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
S08	Infraestructuras	Gestión de obras en diversas infraestructuras municipales	Obras menores en el municipio	Gestión de solicitudes, realización obras menores
			Alcantarillado	Gestión de solicitudes de alcantarillado y reparaciones

2.3 Servicios prestados por las Entidades Locales Menores

A continuación, se describen los **servicios que pueden prestar las Entidades Locales Menores** (caseríos, parroquias, aldeas, barrios, anteiglesias, juntas vecinales o concejos, pedanías, lugares, anejos o parroquias rurales, etc.). Si bien existe una casuística variada de este tipo de entidades y de los servicios, se toma como referencia el contenido del artículo 38 del Real Decreto Legislativo 781/1986, de 18 de abril, por el que se aprueba el texto refundido de las disposiciones legales vigentes en materia de Régimen Local.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que podrían incluirse en cada servicio	INFORMACIÓN IDENTIFICADA

S01	Reparación de infraestructuras	La construcción, conservación y reparación de fuentes, lavaderos y abrevaderos	N/A	**Expedientes de obras solicitudes de reparación**
S02	Control de espacios públicos	La policía de caminos rurales, montes, fuentes y ríos	N/A	**Gestión de permisos de paso y control**
S03	Gestión medioambiental	La limpieza de calles	N/A	**Expedientes de obras solicitudes de reparación** **Solicitudes** **Control y gestión de aprovechamientos comunales**
		La mera administración y conservación de su patrimonio, incluido el forestal, y la regulación del aprovechamiento de sus bienes comunales	N/A	
S04	Obras menores	La ejecución de obras y la prestación de servicios comprendidos en la competencia municipal	N/A	**Expedientes de obras solicitudes de reparación**

2.4 Servicios prestados por Ayuntamientos (o agrupaciones) de hasta 5.000 habitantes con valoración más elevada en alguna de sus dimensiones

En este apartado, se relacionan a modo de ejemplo, servicios valorados en algunas de sus dimensiones de nivel medio/alto.

2.4.1 Servicios de competencia municipal

A continuación, se describen aquellos servicios que pueden prestar los Ayuntamientos (o agrupaciones de estos) cuya valoración en alguna de sus dimensiones puede ser media/alta, por disponer de especiales requisitos sobre la confidencialidad, integridad o autenticidad o por tratarse categorías especiales de datos según la legislación que los regula.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que podrían incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
S09	Padrón de habitantes	Gestión del Padrón	No aplica subservicio	**Altas, bajas y modificaciones**
S10	Servicios sociales de primera intervención	Asistencia urgente	No aplica subservicio	**Expedientes de gestión de ayudas de primera intervención con personas del municipio**

2.4.2 Servicios de competencia municipal incluidos con los anexos I y II de la Directiva NIS2

A continuación, se describen los servicios prestados por las Entidades Locales de pequeño tamaño que se encuentran incluidos[1] en los anexos I y II de la Directiva NIS2 y la norma de transposición.

SERVICIO EELL	Descripción del servicio	COD	SERVICIOS NIS2	NIS2
Medioambiente Urbano	Gestión de los expedientes relacionados entre otros con la Gestión y tratamiento de residuos	S01	Gestión de residuos	ANEXO II
Abastecimiento de agua potable a domicilio y evacuación y tratamiento de aguas residuales	Abastecimiento de agua y saneamiento que garantiza el consumo de agua en los hogares. (El ciclo se inicia con la captación y potabilización del agua, posteriormente es distribuida para su consumo y finalmente, las aguas residuales son depuradas en la EDAR para que puedan ser devueltas al río sin contaminar)	S02	Gestión agua potable	ANEXO I
		S03	Gestión aguas residuales	ANEXO I
Tráfico, estacionamiento de vehículos y movilidad. Transporte colectivo urbano	Gestión del área de tráfico (multas, alegaciones, pago) y del transporte público	S04	Transporte por carretera: autoridades viarias	ANEXO I

A continuación, se detallan los servicios e información.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que podrían incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
S01	Gestión de residuos	Recogida, el transporte, la valorización y la eliminación de los residuos, incluida la vigilancia de estas operaciones, así como el mantenimiento posterior al cierre de los vertederos	No aplica subservicio	**Gestión de expedientes relacionados con el servicio**

[1] Aunque ciertos servicios puedan estar incluidos en los Anexos I y II de NIS2, esto no implica necesariamente que la entidad quede bajo su alcance, ya que factores adicionales, como el tamaño de la población u otros criterios, también determinan dicha aplicabilidad.

COD	SERVICIO ALCANCE PCE	Descripción del servicio	Descripción SUB-SERVICIOS que podrían incluirse en cada servicio	INFORMACIÓN IDENTIFICADA
S02	Agua potable	Suministradores y distribuidores de aguas destinadas al consumo humano	No aplica subservicio	Gestión de expedientes relacionados con el servicio
S03	Alcantarillado	Recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales	No aplica subservicio	Gestión de expedientes relacionados con el servicio
S04	Transporte por carretera: autoridades viarias	Planificación, el control o la gestión de las carreteras en el ámbito territorial de su competencia; control de la gestión del tráfico	No aplica subservicio	Información sobre la gestión del tráfico y videovigilancia

3. CONSIDERACIONES DEL SISTEMA DE INFORMACIÓN

En el ámbito de la seguridad de la información, las entidades locales presentan distintos contextos tecnológicos en función de su tamaño, sus competencias, su modelo de prestación de servicios y la naturaleza de los sistemas que soportan su actividad. Esta diversidad tiene un impacto directo en el enfoque y el alcance que deben adoptarse en el proceso de adecuación al Esquema Nacional de Seguridad (ENS).

Por un lado, existen entidades locales cuyo sistema de información se sustenta exclusivamente en infraestructuras de tecnologías de la información (IT). En estos casos, los activos que deben protegerse están compuestos fundamentalmente por sistemas corporativos, aplicaciones de gestión municipal, sedes electrónicas, portales y servicios digitales, redes de comunicaciones y plataformas tecnológicas orientadas a la tramitación administrativa y al tratamiento de la información.

Por otro lado, determinadas entidades locales disponen de sistemas de información que no se limitan al ámbito IT, sino que incorporan también infraestructuras de tecnologías de operación (OT) y tecnologías del Internet de las cosas (IoT). Estas tecnologías pueden resultar necesarias para la gestión, supervisión y prestación de servicios municipales que interactúan con infraestructuras, dispositivos conectados o procesos físicos.

En estos casos, los sistemas IT conviven e interactúan con:

- Entornos OT, industriales, operacionales o de control, integrados, entre otros elementos, por sistemas SCADA, autómatas programables (PLC), sistemas de supervisión, estaciones de control, sensores, actuadores y redes de control o industriales. Su finalidad es monitorizar, controlar u operar procesos físicos vinculados a la prestación de servicios municipales. Entre otros, pueden encontrarse en las instalaciones de abastecimiento y distribución de agua potable, saneamiento y tratamiento de aguas residuales, gestión del tráfico,

túneles e infraestructuras viarias, alumbrado público, instalaciones energéticas municipales, sistemas de bombeo, estaciones depuradoras, gestión de residuos o instalaciones y edificios municipales. Los servicios de abastecimiento de agua, saneamiento, gestión de residuos y control del tráfico forman parte de los servicios contemplados para las entidades locales en el punto anterior.

- Entornos IoT, formados por dispositivos, sensores, actuadores, elementos de comunicación, pasarelas y plataformas conectadas que permiten captar información, intercambiar datos, supervisar condiciones o actuar sobre el entorno físico. En el ámbito municipal, estas tecnologías pueden utilizarse, entre otros, en proyectos de ciudad inteligente (*smart city*), sistemas de alumbrado inteligente, estacionamiento conectado, regulación y monitorización del tráfico, control ambiental y de la calidad del aire, gestión inteligente de residuos, telelectura de contadores, riego de parques y jardines, control de aforos, videovigilancia, edificios inteligentes o supervisión remota de infraestructuras y equipamientos municipales.

La incorporación de tecnologías OT e IoT da lugar a entornos municipales convergentes IT/OT/IoT, en los que los sistemas de gestión y las redes corporativas interactúan con dispositivos conectados, infraestructuras operacionales y procesos físicos. Las particularidades de estos entornos podrán requerir la adaptación de la forma en que se implantan determinadas medidas de seguridad, sin menoscabar el cumplimiento de los objetivos del ENS ni el nivel de protección exigido.

Este escenario convergente introduce una complejidad adicional relevante desde el punto de vista del ENS, ya que:

- El sistema de información que debe protegerse puede incluir sistemas corporativos, aplicaciones de gestión, dispositivos conectados, infraestructuras municipales y procesos físicos asociados a la prestación de servicios públicos.
- La protección debe extenderse a la continuidad y al comportamiento seguro de los procesos OT, de los dispositivos y servicios IoT y de los servicios municipales soportados por dichos activos.
- La categorización y el análisis de riesgos deben considerar no solo las consecuencias sobre la información y los servicios digitales, sino también los posibles efectos sobre la prestación efectiva del servicio municipal, las infraestructuras físicas, las personas y el entorno.
- Existen requisitos adicionales de disponibilidad, continuidad operativa, resiliencia y seguridad física que, en determinados servicios municipales, pueden resultar especialmente relevantes. Entre estos servicios se encuentran el abastecimiento de agua potable, el saneamiento, la gestión de residuos y la planificación y el control del tráfico.
- La exposición al riesgo se amplía como consecuencia de la convergencia IT/OT/IoT, al aumentar la superficie de exposición y generarse nuevos vectores de ataque, interconexiones y dependencias cruzadas entre las redes

corporativas, las plataformas de gestión, los dispositivos conectados y las infraestructuras operacionales.

- Se requiere adaptar los controles de seguridad a entornos en los que las actualizaciones, los cambios de configuración, las pruebas o las medidas de protección pueden afectar directamente al funcionamiento de los dispositivos, a la operación de las infraestructuras o a la continuidad de los servicios municipales.
- Deben considerarse las dependencias respecto de proveedores, concesionarios, empresas de mantenimiento y prestadores externos que participen en la gestión de las plataformas, dispositivos e infraestructuras OT e IoT utilizadas para prestar servicios municipales.
- La implantación de las medidas de seguridad deberá preservar la seguridad, la estabilidad, la disponibilidad y la continuidad de los procesos OT y de los servicios o procesos físicos soportados por tecnologías IoT. Deberá evitarse que la aplicación de un control de seguridad introduzca un riesgo operacional superior al riesgo que pretende mitigar.
- La adecuación al ENS deberá contemplar una visión integral del servicio municipal, incluyendo los sistemas IT, OT e IoT que lo soportan, sus interconexiones, sus dependencias tecnológicas y los efectos que un incidente de seguridad podría producir sobre la población y sobre la prestación de los servicios públicos locales.

Los ejemplos indicados no constituyen una relación cerrada. La consideración de un activo o sistema como IT, OT o IoT dependerá de su función, su arquitectura, su conectividad y su participación en la prestación del servicio municipal.

4. DECLARACIÓN DE APLICABILIDAD

Teniendo en cuenta la casuística del modelo propuesto se ha determinado que, para garantizar la seguridad de los sistemas concernidos, la relación de medidas del Anexo II del ENS que resultan de aplicación y exigencia en el nivel de seguridad, son las recogidas en la siguiente tabla.

Dado que puede resultar diferente el grado de aplicación del control si el alcance contempla servicios respaldados por tecnologías de la información (IT) o contempla servicios respaldados tanto por tecnologías de la información (IT) como por tecnologías de operación (OT) o del internet e las cosas (IoT), se presenta una separación en la tabla de medidas aplicables.

El "*" indica que la medida en cuestión requiere de unos criterios específicos de aplicación, que se detallan en el apartado "**4. CRITERIOS DE APLICABILIDAD DE MEDIDAS**".

Dimensiones Afectadas	CAT B	CAT M	CAT A	Control	Aplicación IT[2]	Aplicación IT/OT/IoT[3]	Ref *
Categoría	aplica	aplica	Aplica	org.1	BÁSICA	BÁSICA	
Categoría	aplica	aplica	Aplica	org.2	BÁSICA	BÁSICA	
Categoría	aplica	aplica	Aplica	org.3	BÁSICA	BÁSICA	
Categoría	aplica	aplica	Aplica	org.4	BÁSICA	BÁSICA	
Categoría	aplica	+ R1	+ R2	op.pl.1	BÁSICA	BÁSICA	**5.1**
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	N/A	N/A	
Categoría	aplica	aplica	Aplica	op.pl.3	BÁSICA	BÁSICA	
D	aplica	+ R1	+ R1	op.pl.4	N/A	N/A	
Categoría	n.a.	aplica	Aplica	op.pl.5	N/A	N/A	
T A	aplica	+ R1	+ R1	op.acc.1	BAJO	BAJO	
C I T A	aplica	aplica	+ R1	op.acc.2	BAJO	BAJO	
C I T A	n.a.	aplica	+ R1	op.acc.3	N/A	N/A	
C I T A	aplica	aplica	Aplica	op.acc.4	BAJO	BAJO	
C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	op.acc.5	BAJO	BAJO	
C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	op.acc.6	BAJO	BAJO	**5.2**
Categoría	aplica	aplica	Aplica	op.exp.1	BÁSICA	BÁSICA	**5.3**
Categoría	aplica	aplica	Aplica	op.exp.2	BÁSICA	BÁSICA	
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	N/A	N/A	
Categoría	aplica	+ R1	+ R1 + R2	op.exp.4	BÁSICA	BÁSICA	**5.4**
Categoría	n.a.	aplica	+ R1	op.exp.5	N/A	MEDIA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	BÁSICA	BÁSICA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	BÁSICA	BÁSICA	**5.5**
T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	BAJO	BAJO	**5.6**
Categoría	aplica	aplica	Aplica	op.exp.9	N/A (*)	N/A (*)	**5.7**
Categoría	aplica	+ R1	+ R1	op.exp.10	BÁSICA	BÁSICA	
Categoría	n.a.	aplica	Aplica	op.ext.1	N/A	N/A	
Categoría	n.a.	aplica	Aplica	op.ext.2	N/A	N/A	
Categoría	n.a.	n.a.	Aplica	op.ext.3	N/A (*)	N/A (*)	**5.8**

[2] En la columna "Aplicación IT", se reflejará la categoría (BÁSICA, MEDIA, ALTA) que se aplicará en caso de entidades cuyo alcance contemple servicios respaldados por tecnologías de la información (IT). Se refleja la categoría que corresponda en caso de que en esa medida se vean afectadas las cinco (5) dimensiones de seguridad (Confidencialidad-C, Integridad-I, Autenticidad-A, Trazabilidad-T, Disponibilidad-D). En caso, de que no se vean afectadas las cinco (5) dimensiones, se reflejará el nivel a aplicar (BAJO, MEDIO, ALTO).

[3] En la columna "Aplicación IT/OT/IoT", se reflejará la categoría (BÁSICA, MEDIA, ALTA) que se aplicará en caso de entidades cuyo alcance contemple servicios respaldados tanto por tecnologías de la información (IT) como por tecnologías de operación (OT) o del internet e las cosas (IoT). Se refleja la categoría (BÁSICA, MEDIA, ALTA) que corresponda en caso de que en esa medida se vean afectadas las cinco (5) dimensiones de seguridad (Confidencialidad-C, Integridad-I, Autenticidad-A, Trazabilidad-T, Disponibilidad-D). En caso, de que no se vean afectadas las cinco (5) dimensiones, se reflejará el nivel a aplicar (BAJO, MEDIO, ALTO).

Dimensiones Afectadas	CAT B	CAT M	CAT A	Control	Aplicación IT[2]	Aplicación IT/OT/IoT[3]	Ref *
Categoría	n.a.	aplica	+ R1	op.ext.4	N/A	N/A	
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	N/A	N/A	
D	n.a.	aplica	Aplica	op.cont.1	N/A	N/A	
D	n.a.	n.a.	Aplica	op.cont.2	N/A (*)	N/A (*)	5.9
D	n.a.	n.a.	Aplica	op.cont.3	N/A	N/A	
D	n.a.	n.a.	Aplica	op.cont.4	N/A	N/A	
Categoría	aplica	+ R1	+ R1 + R2	op.mon.1	N/A	BÁSICA	
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	BÁSICA	BÁSICA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	N/A	N/A	
Categoría	aplica	aplica	Aplica	mp.if.1	BÁSICA	BÁSICA	5.10
Categoría	aplica	aplica	Aplica	mp.if.2	N/A	BÁSICA	5.11
Categoría	aplica	aplica	Aplica	mp.if.3	N/A	N/A	
D	aplica	+ R1	+ R1	mp.if.4	N/A	N/A	
D	aplica	aplica	Aplica	mp.if.5	N/A	N/A	
D	n.a.	aplica	Aplica	mp.if.6	N/A	N/A	
Categoría	aplica	aplica	Aplica	mp.if.7	N/A	N/A	
Categoría	n.a.	aplica	Aplica	mp.per.1	N/A	N/A	
Categoría	aplica	+ R1	+ R1	mp.per.2	BÁSICA	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.per.3	BÁSICA	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.per.4	BÁSICA	BÁSICA	
Categoría	aplica	+ R1	+ R1	mp.eq.1	BÁSICA	BÁSICA	
A	n.a.	aplica	+ R1	mp.eq.2	MEDIO	MEDIO	
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	BÁSICA	BÁSICA	
C	aplica	+ R1	+ R1	mp.eq.4	BAJO	BAJO	
Categoría	aplica	aplica	Aplica	mp.com.1	BÁSICA	BÁSICA	5.12
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	BAJO	BAJO	
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	N/A	N/A	
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	N/A	MEDIA	
C	n.a.	aplica	Aplica	mp.si.1	N/A	N/A	
C I	n.a.	aplica	+ R1 + R2	mp.si.2	N/A	N/A	
Categoría	aplica	aplica	Aplica	mp.si.3	BÁSICA	BÁSICA	
Categoría	aplica	aplica	Aplica	mp.si.4	BÁSICA	BÁSICA	
C	aplica	+ R1	+ R1	mp.si.5	BAJO	BAJO	
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	N/A	N/A	
Categoría	aplica	+ R1	+ R1	mp.sw.2	N/A	N/A	
Categoría	aplica	aplica	Aplica	mp.info.1	BÁSICA	BÁSICA	
C	n.a.	aplica	Aplica	mp.info.2	N/A	N/A	
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	BAJO	BAJO	
T	n.a.	n.a.	Aplica	mp.info.4	N/A	N/A	
C	aplica	aplica	Aplica	mp.info.5	BAJO	BAJO	
D	aplica	+ R1	+ R1 + R2	mp.info.6	BAJO	BAJO	5.13
Categoría	aplica	aplica	Aplica	mp.s.1	BÁSICA	BÁSICA	
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	N/A	N/A	
Categoría	aplica	aplica	+ R1	mp.s.3	BÁSICA	BÁSICA	
D	n.a.	aplica	+ R1	mp.s.4	N/A	N/A	

Detalles del criterio específico de aplicación de la media en el apartado 4 de este documento

Se considera que la medida no será de aplicación al PCE RFS

4.1 MEDIDAS DE APLICACIÓN

De las 73 medidas de seguridad definidas en el Anexo II del ENS, **aplican un total de 38*[4] medidas** en aquellas entidades cuyo alcance contemple servicios respaldados por tecnologías de la información (IT). En el caso de entidades cuyo alcance contemple servicios respaldados tanto por tecnologías de la información (IT) como por tecnologías de operación (OT) o del internet e las cosas (IoT), **el número de medidas aplicables asciende a 42*[4]**.

La distribución de las medidas aplicables por ámbito de control es la siguiente:

- Marco Organizativo: 4 medidas.
- Marco Operacional: 15 medidas para entorno IT y 17 para entorno convergente IT/OT/IoT.
- Medidas de Protección: 19 medidas para entorno IT y 21 para entorno convergente IT/OT/IoT.

Marco Organizativo:

[org.1] Política de seguridad

[org.2] Normativa de seguridad

[org.3] Procedimientos de seguridad

[org.4] Proceso de autorización

Marco Operacional:

[op.pl] Planificación

[op.pl.1] Análisis de riesgos

[op.pl.3] Adquisición de nuevos componentes

[op.acc] Control de acceso

[op.acc.1] Identificación

[op.acc.2] Requisitos de acceso

[op.acc.4] Proceso de gestión de derechos de acceso

[op.acc.5] Mecanismo de autenticación (usuarios externos)

[op.acc.6] Mecanismo de autenticación (usuarios de la organización)

[4] Número aproximado de medidas que aplican

[op.exp] Explotación
[op.exp.1] Inventario de activos
[op.exp.2] Configuración de seguridad
[op.exp.4] Mantenimiento y actualizaciones de seguridad
[op.exp.5] Gestión de cambios[5]
[op.exp.6] Protección frente a código dañino
[op.exp.7] Gestión de incidentes
[op.exp.8] Registro de la actividad
[op.exp.10] Protección de claves criptográficas
[op.mon] Monitorización del sistema
[op.mon.1] Detección de intrusión[5]
[op.mon.2] Sistema de métricas

Medidas de Protección

[mp.if] Protección de las instalaciones e infraestructuras
[mp.if.1] Áreas separadas y control de acceso
[mp.if.2] Identificación de las personas[5]
[mp.per] Gestión del personal
[mp.per.2] Deberes y obligaciones
[mp.per.3] Concienciación
[mp.per.4] Formación
[mp.eq] Protección de los equipos
[mp.eq.1] Puesto de trabajo despejado
[mp.eq.2] Bloqueo de puesto de trabajo
[mp.eq.3] Protección de dispositivos portátiles
[mp.eq.4] Otros dispositivos conectados a la red.
[mp.com] Protección de las comunicaciones
[mp.com.1] Perímetro seguro

[5] La medida aplica a las entidades cuyo alcance contemple servicios respaldados tanto por tecnologías de la información (IT) como por tecnologías de operación (OT) o del internet e las cosas (IoT).

[mp.com.2] Protección de la confidencialidad

[mp.com.4]Separación de flujos de información en la red[6]

[mp.si] Protección de los soportes de información

[mp.si.3] Custodia

[mp.si.4] Transporte

[mp.si.5] Borrado y destrucción

[mp.info] Protección de la información

[mp.info.1] Datos de carácter personal

[mp.info.3] Firma electrónica

[mp.info.5] Limpieza de documentos

[mp.info.6] Copias de seguridad (backup)

[mp.s] Protección de los servicios

[mp.si.1] Protección del correo electrónico

[mp.s.3] Protección de la navegación web

5. CRITERIOS DE APLICABILIDAD DE MEDIDAS

5.1 [op.pl.1] Análisis de riesgos

Automatizado en el Portal de Gobernanza (https://gobernanza.ccn-cert.cni.es/). Para su desarrollo se han analizado las necesidades de seguridad, los recursos que se disponen y contemplando las vulnerabilidades y amenazas a las que se ven expuestos los sistemas.

Se tendrán en cuenta también los potenciales riesgos derivados de la IA ofensiva.

5.2 [op.acc.6] Mecanismo de autenticación (usuarios de la organización)

Se recomienda que, aunque el acceso al equipo se realice desde una zona controlada[7], se implemente el Refuerzo R2 – Contraseña más otro factor de autenticación (múltiple factor de autenticación –MFA–), con el fin de incrementar el nivel de protección frente a accesos no autorizados, especialmente en aquellas entidades que presten alguno de los servicios enumerados en los Anexos I y II de la Directiva NIS2 (véase apartado del

[6] La medida aplica a las entidades cuyo alcance contemple servicios respaldados tanto por tecnologías de la información (IT) como por tecnologías de operación (OT) o del internet e las cosas (IoT).

[7] Se entiende por zona controlada aquella en la que al usuario se le ha requerido una autenticación previa, mediante un control de acceso formalizado a las instalaciones, y en la que se han aplicado los requisitos de seguridad necesarios antes de permitir el acceso al equipo.

presente PCE "2.4.2 Servicios de competencia municipal incluidos con los anexos I y II de la Directiva NIS2").

5.3 [op.exp.1] Inventario de activos

[Aplicación IT/OT/IoT]:

Se implementará el Refuerzo voluntario R3 – Identificación de activos críticos, con el fin de poder categorizar los activos críticos por contexto de la organización y riesgos de seguridad.

5.4 [op.exp.4] Mantenimiento y actualizaciones de seguridad

[Aplicación IT/OT/IoT]:

En el contexto OT, se implementará el Refuerzo R1 – Pruebas en preproducción. Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

5.5 [op.exp.7] Gestión de incidentes

Especialmente en aquellas entidades que presten alguno de los servicios enumerados en los Anexos I y II de la Directiva NIS2, se recomienda la implantación del Refuerzo R1 – Notificación, con el fin de disponer de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

5.6 [op.exp.8] Registro de la actividad

Los eventos y actividades de los usuarios requeridos serán la de los usuarios en los servidores.

5.7 [op.exp.9] Registro de la gestión de incidentes

En el caso de que las entidades a las que sea de aplicación el presente PCE presten alguno de los servicios enumerados en los Anexos I y II de la Directiva NIS2 (véase apartado del presente PCE "2.4.2 Servicios de competencia municipal incluidos con los anexos I y II de la Directiva NIS2"), se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

5.8 [op.ext.3] Protección de la cadena de suministro

En el caso de que las entidades a las que es de aplicación el presente PCE presten alguno de los servicios enumerados en los Anexos I y II de la Directiva NIS2, se identificarán y evaluarán los riesgos asociados a proveedores, productos y servicios externos que

formen parte de la cadena de suministro, adoptando las medidas necesarias para prevenir, mitigar y contener los impactos que un incidente en dichos elementos pudiera ocasionar sobre el sistema de información.

Para apoyar a cada organismo, entidad u organización en sus procesos de contratación, se ofrecen la guía 'CCN-STIC-890 Anexo VI. Cuestionario de protección de cadena de suministro', disponible también de forma automatizada en la Plataforma de Gobernanza.

Estos documentos facilitan que los servicios y productos contratados cumplan con el Artículo 2 del RD 311/2022, que regula el ENS y estén alineados con Directiva (UE) 2022/2555 (NIS2).

5.9 [op.cont.2] Plan de continuidad

En el caso de que las entidades a las que sea de aplicación el presente PCE presten alguno de los servicios enumerados en los Anexos I y II de la Directiva NIS2 (véase apartado del presente PCE "2.4.2 Servicios de competencia municipal incluidos con los anexos I y II de la Directiva NIS2") se deberán implementar mecanismos efectivos de continuidad que garanticen la disponibilidad y resiliencia de dichos servicios ante incidentes que puedan comprometer su operatividad.

El modelo de referencia para el desarrollo de estos planes puede encontrarse en la Guía CCN-STIC-890 Anexo IV. Plan de Continuidad, el cual debe ser adaptado por cada entidad según su estructura y necesidades específicas. Este modelo proporciona una base para diseñar e implementar un plan de continuidad robusto, abarcando todas las acciones necesarias para garantizar que los servicios esenciales puedan mantenerse operativos o recuperarse en el menor tiempo posible.

5.10 [mp.if.1] Áreas separadas y control de acceso

En caso de que no se disponga de Centro de Proceso de Datos (CPD), el equipamiento se instalará, en la medida de lo posible, en áreas que aseguren que solo el personal autorizado tenga acceso a ellas.

[Aplicación IT/OT/IoT]:

Además del acceso al CPD, se controlarán los accesos a salas de control y centros de operación, armarios y cuadros de automatización, centros de transformación y sistemas auxiliares críticos, sistemas instrumentados de seguridad (SIS) e infraestructuras OT/IoT remotas, dónde el acceso físico puede traducirse directamente en un compromiso de la operación.

5.11 [mp.if.2] Identificación de las personas

[Aplicación IT/OT/IoT]:

Además de la identificación de las personas que acceden al CPD, se tendrá dicha identificación en cuenta en las ubicaciones donde se encuentren salas de control y centros de operación, armarios y cuadros de automatización, centros de transformación

y sistemas auxiliares críticos, sistemas instrumentados de seguridad (SIS) e infraestructuras OT/IoT remotas, dónde el acceso físico puede traducirse directamente en un compromiso de la operación.

5.12 [mp.com.1] Perímetro Seguro

En caso de que no exista red, los equipos tendrán configurado el *firewall* del sistema operativo.

5.13 [mp.info.6] Copias de seguridad

Para dar cumplimiento a los requisitos de la medida para nivel BAJO y al artículo 26. Continuidad de la actividad, se dispondrá de al menos una copia de seguridad actualizada, almacenada en una ubicación diferente a la del sistema principal, que garantice su disponibilidad en caso de incidente. Dicha copia podrá ser *offline* (física) y/o en una ubicación remota (lógica) segura.